# CHAPTER 8
# INVESTING IN SPACE, INFORMATION AND INTELLIGENCE

The Department has made significant efforts to improve capabilities in Space, Information and Intelligence (SII) to help mitigate future risks and is committed to doing more. These initiatives enhance the flexibility of our forces and their capacity to meet a wider range of contingencies. SII contributes directly to meeting all six of the QDR's operational goals. SII enhancements are increasing the speed of operations and reducing cycle times, allowing decisions to be made at proper levels, and fusing information and intelligence flows. They have made demonstrable contributions already in the global war on terrorism.

## *SII Objectives*

DoD's space, information, and intelligence activities will focus on:

- Enhancing the capability, accessibility, and survivability of space systems;
- Providing a secure, high capacity, dependable global network;
- Populating the network with high quality information and intelligence to achieve global situational awareness and support network-centric warfare; and
- Making SII systems more robust and secure while denying similar capabilities to adversaries.

## *Space Systems*

Last year the Commission to Assess United States National Security Space Management and Organization (Space Commission) observed:

> *"The security and economic well being of the United States and its allies and friends depend on the nation's ability to operate successfully in space. . . .*

*Specifically, the U.S. must have the capability to use space as an integral part of its ability to manage crises, deter conflicts and, if deterrence fails, to prevail in conflict."*

DoD is making organizational changes in response to the Space Commission's recommendations, for example, by consolidating space responsibilities with the Under Secretary of the Air Force. The nation is taking other steps in light of our increasing dependency on space. It also requires that the government develop commercial partnerships, and maximize dual-use capabilities and exploit commercial systems for military use to serve as a springboard to accelerate and improve military space capabilities. Military space capabilities fall into the following key areas:

- Space launch, range operations, and terrestrial control networks;
- Intelligence, surveillance, reconnaissance (ISR);
- Satellite communications (SATCOM);
- Launch detection and tracking;
- Navigation and force tracking;
- Meteorology and other environmental support to military operations; and
- Space surveillance and control.

The President's Budget and associated FYDP support important programs in each of these areas that are necessary to execute our strategy. About $200 million is being proposed for new space-related transformation programs in FY 2003, with significantly more planned in the future.

***Space Launch, Range Operations, and Terrestrial Control Networks.*** As legacy space launch systems are flown out, the Department is partnering with industry to develop a rapid launch capability more responsive to warfighter and civil requirements. Development of the Evolved Expendable Launch Vehicle (EELV) will provide medium- and heavy-lift launch capabilities at reduced cost. First launch of the medium-lift variant is scheduled for 2002, with the heavy-lift capability in 2003. The Eastern and Western launch ranges, vital to civil and military space operations, are undergoing overdue upgrades. Partnering with industry, the Department is

developing innovative solutions to reducing launch infrastructure and operations costs, while expanding capabilities.

***Intelligence, Surveillance, Reconnaissance (ISR).*** The Department provides detailed imagery intelligence (IMINT), signals intelligence (SIGINT), and measurement and signature intelligence (MASINT) capabilities supporting both decision makers and worldwide military operations. Space plays a critical role in many of these. The FY 2003 President's budget includes investments to improve the quality and quantity of imagery and other intelligence. One example is the Space-Based Radar, which will provide the capability to detect and track moving ground targets from space.

***Satellite Communications (SATCOM) Capabilities.*** The Department continues to leverage commercial systems and developing technologies. The importance of leveraging commercial technology and services was demonstrated in Afghanistan. DoD was able to lease transponders on commercial satellites to extend communications reach and increase bandwidth and to distribute commercial SATCOM handsets with secure appliques to provide augmented mobile communications capabilities in the theater of operations. DoD also was able to accelerate the purchase and deployment of survivor location radios. Major SATCOM improvements are programmed over the FYDP, including satellites with complementary capabilities designed to increase greatly secure bandwidth to the warfighter and provide improved resistance to electronic jamming.

***Launch Detection and Tracking.*** Ballistic missile launch detection and warning are capabilities essential to providing tactical warning of attack by long- and short-range missiles. That warning is essential to cueing responses, including missile defenses. These capabilities are currently provided by the Defense Support Program satellites and ground-based early warning radar systems. The budget assures these capabilities will be preserved in the near term and improved in the future. The budget also funds the Satellite Sensor Technology program that is aimed at developing a range of technologies applicable to space-based detection, tracking, and discrimination support for missile defense.

***Navigation and Force Tracking***. The Department provides worldwide precision position, navigation, and timing to both military and civilian users using the highly successful Global Positioning System (GPS) satellite constellation. Scheduled for launch beginning in October 2005, an upgraded generation of GPS satellites, Block IIF, will fulfill Presidential guidance by adding a second civil frequency for all users. The budget also supports development of fourth-generation satellites, GPS III, designed to increase signal power and accuracy greatly.

***Meteorology and other Environmental Support to Military Operations***. Weather is a critical factor in military operations, and space systems are essential in helping the warfighter predict and understand it. The Department has a series of modernization programs underway with other government agencies, plus commercial and international partners, to improve our environmental support to the operating forces.

***Space Surveillance and Control.*** A key objective of the Department's space surveillance and control mission is to ensure freedom of action in space for the United States and its allies and, when directed, deny such freedom of action to adversaries. To enhance the capabilities of the ground-based space surveillance network, the Department is developing a space-based space surveillance system designed to identify and track satellites and debris, and provide warning or potentially hostile action against U.S. satellites or those of allies and friends.

## *Global Network*

DoD's network strategy is to leverage the power of emerging information technology and concepts to provide seamless, secure, wide-band connectivity and interoperability. Three goals will focus our efforts in the coming years: (1) extending the reach of our communications infrastructure to all elements of the force; (2) maximizing interoperability between Intelligence networks and DoD's integrated network; and (3) eliminating bandwidth as a constraint. The 2003 budget requests $2.3 billion to leverage information technology and associated transformational programs.

***Global Information Grid (GIG).*** The GIG is an enterprise information technology (IT) architecture that includes coverage for all Joint mission

areas, continuity of operations (COOP), Homeland Security and Defense, and all business processes. The end goal is the delivery of secure, assured, effective, and interoperable information services to the warfighter and agencies that support national security. Three critical enterprise services will be leveraged: network operations, information assurance, and information dissemination.

***ISR-Operational Integration.*** All phases of the information cycle will be integrated with operational decision-making and weapons systems processes. For example, in Afghanistan, real-time imagery from Predator UAVs, integrated with GPS positioning information, was datalinked to aircraft enabling them to strike high priority, emerging targets in minutes rather than hours or days. Additional efforts are underway to streamline the process in support of all-weather, precision strike of time-critical targets. Technology efforts, such as DARPA's Affordable Moving Surface Target Engagement demonstration, are focused on integrating the necessary ISR and weapon systems elements into an integrated reconnaissance-strike complex.

## *Intelligence Initiatives*

The weeks following September 11 highlight the intelligence challenges the nation faces in a world of surprise and asymmetric capabilities. The Department must transform its information and intelligence approach to meet the challenge. Two trends drive this transformation. First, as a consequence of the expanded range of missions the U.S. military is undertaking and numerous geographic locales in which it must operate, new types of information and different perspectives must be brought to bear. This requires that DoD ensure useful sources of information remain accessible. Second, information flows have become and will continue to be separated from the chain of command. Together, these trends are creating a proliferation of information sources and a fundamental change in the way information is distributed and utilized.

The resulting challenges to U.S. national security are manifold. First, the information needs of U.S. forces are less predictable and more dynamic than ever. Second, although more data will be collected, deriving valuable information required by combat commanders and policy makers will be

made difficult by the sheer volume of intelligence and continued demand for its timely reporting. Third, the United States will require robust intelligence analysis capabilities, bringing together individuals with varying perspectives and expertise to assess the available intelligence. As U.S. military concepts of operation become more and more dependent upon information, success will require placing a premium on information collection, information sharing, and collaborative intelligence processes. The United States must place more emphasis on rapidly analyzing collected data to support advanced warning, responsive decision-making, and operational forces. In addition, predictive analysis vital to supporting the long lead times required by acquisition programs and force structure development will be critical to enabling successful Departmental transformation. Transformation also requires the United States to make a fundamental change from its current push-oriented tracking, processing, exploitation, and dissemination process to a pull-oriented, collaborative process with a "post before use" policy. The goal is to provide networked, responsive intelligence capable of surprising and countering U.S. adversaries through persistent and relentless coverage and a set of robust, resilient, and hardened defense capabilities.

Many initiatives can take advantage of the global network. For example, the Joint Worldwide Intelligence Communications System, the Joint Deployable Intelligence Support System, and the Joint Intelligence Virtual Architecture are making it possible for intelligence and operations professionals in geographically separated locations and on different time schedules to view the same digital imagery and map products, collaborate on targeting activities, review battle damage assessment information, and generate rapid re-strike nominations over secure networks.

As the global network is built, it must be populated with quality information. Such information is the result of collecting the right data and being able to make the data available to a variety of users, to be processed and fused in different ways for different purposes as their needs dictate. This information includes not only intelligence about adversaries, but also friendly force content, such as locating data, personnel, medical, and logistics updates, financial management, and e-business approaches. The President's budget requests $3.3 billion for transformational information and intelligence programs. Some of the initiatives include:

***Imagery.*** DoD and the Intelligence Community are developing the Geo-Spatial Intelligence (GSI) System to provide commanders and other military intelligence consumers better imagery support. GSI will make imagery and related products and services faster, more responsive, and less complex for the user by posting images to the network immediately for access by the entire set of users.

***Signals Intelligence (SIGINT).*** The rapidly increasing volume and complexity of modern communications signals poses a daunting but crucial challenge for the US SIGINT system. While the challenge is ever more difficult, the benefits when success is achieved are also enormous. The Defense Department will continue to make the health and viability of SIGINT as high priority element of transformation.

***New Collection Capabilities.*** A wide variety of new collection capabilities is becoming operational or is in various phases of acquisition. Spaceborne systems in the Future Imagery Architecture, Integrated Overhead SIGINT Architecture, Space-Based Infrared System, and Space-Based Radar will provide worldwide access to many new targets, as well as traditional ones. Improvements to the U-2 radar and electro-optical systems are being fielded. Advanced sensor phenomenologies are being demonstrated to improve detection capabilities. The Radar Technology Improvement Program will provide significantly increased capability for the Joint Surveillance Target Attack Radar System (JSTARS) and the Global Hawk Unmanned Air Vehicle (UAV) systems. Commercial satellite imagery is also being used to complement national collection capabilities. A modernization plan has been developed for Measurement and Signature Intelligence (MASINT) to invigorate MASINT capabilities and integrate them with other intelligence disciplines.

***Intelligence, Surveillance, Reconnaissance (ISR) Integration.*** The Department will integrate systems across the space, air, land, and sea domains to make best use of the complementary capabilities in each area. Transformational concepts, such as automated sensor cross-cueing, are beginning to transition from laboratory tests into system development efforts. For example, the Airborne Targeting and Cross-Cueing System employs risk-reduction activities aimed at automatically linking existing

and planned airborne radar, electro-optical and signals collection sensor control and exploitation systems. This will provide needed links between wide-area battlefield surveillance technologies (moving target indication, wide-area radar imagery coverage, and signals collection) and reconnaissance capabilities (high-resolution electro-optical and radar imagery), while providing target identification aids to the intelligence analysts exploiting the resultant multi-source collections.

***Integrating Other Kinds of Information.*** All available information, not just intelligence, must be brought to bear throughout the network. Systems need to be designed so that users only have to handle information once. Producers of information, wherever they may be, need to post what they know, as well as exploiting what others have learned. For example, information gathered by the radars of modern fighters need to be disseminated, just as information is disseminated from intelligence sensors. Electronic business and electronic government initiatives are being integrated across the Federal government. The DoD Chief Information Officer is responsible for ensuring the interoperability of such information as well as the efficient and effective acquisition of the IT systems to support it. Advanced analytical techniques are being developed to make sense out of the overwhelming volumes of information that will be available.

## *Making Space, Information and Intelligence (SII) Systems More Robust and Secure*

The information domain is where warfighters command and control modern joint and coalition military forces and where a commander's intent is conveyed. Consequently, it is a domain that must be protected and defended. In a networked environment, information assurance is critical. A total of $2 billion is provided in FY 2003 to improve the robustness and security of SII systems. This is a 15.6 percent increase over FY 2002.

***Defense-in-Depth.*** DoD's strategy for protecting the infostructure (information infrastructure) is called Defense-in-Depth. It goes beyond defensive perimeter activities, encompassing defenses layered in depth throughout the network enterprise and in breadth across decentralized and distributed network architectures. However, security, like interoperability,

must be engineered into systems from the beginning. The forging of a coherent infostructure out of many legacy systems poses a significant challenge.

To ensure the incorporation of security early in the design of new acquisitions, DoD has modified acquisition regulations to require information assurance strategies for each acquisition program. The strategies are scrutinized at major acquisition milestones and are key considerations for program continuation. Legacy systems are subject to rigorous security certification, and accreditation criteria are required for connection to both classified and unclassified networks. In addition, by July 2002, commercial-off-the-shelf information assurance and information assurance-enabled products must be evaluated against specific assurance criteria prior to purchase.

***Insider Threats.*** A critical focus is creating strategies to mitigate risks that are applicable to personnel, physical and cyber vulnerabilities. Transforming the screening processes and reviews to reduce the backlog of clearance investigations, conducting vulnerability assessments of critical assets, increasing support to counterintelligence and industrial security, as well as leveraging technology are key thrusts. Public Key Infrastructure, high capacity encryption, and intrusion detection programs are notable efforts designed to enhance the confidentiality, authentication, and availability of infostructure services. While many challenges remain in the mitigation of insider threats, DoD systematically continues to secure its infostructure by modernizing its aging cryptographic backbone and other enterprise-wide information assurance initiatives.